TITLE: Situation Report on Warning

AUTHOR: David Y. McManis

VOLUME: 27 ISSUE: Winter YEAR: 1983

STUDIES IN INTELLIGENCE

A collection of articles on the historical, operational, doctrinal, and theoretical aspects of intelligence.

SITUATION REPORT ON WARNING

David Y. McManis

The warning community, both governmental and academic, has spent a great deal of time and effort looking at the warning "failures" of the past, starting with Pearl Harbor and carrying us through the invasion of Czechoslovakia and the fall of the Shah of Iran. While dwelling on past "failures" may be academically instructive and even mildly rewarding, this is 1984, and not 1941, and we as a community have evolved to a degree we probably never anticipated.

One way to understand how far we have come is to get into Ivan's shoes for a look at the current US Warning System as he sees it. (I wish we had a better appreciation of how the Soviets really understand our system, just as I wish we understood their warning system better. The technical components and wiring diagrams are relatively easy but it is much more difficult to understand the cognitive warning process.)

Ivan probably sees:

a. an incredibly sophisticated total system replete with the latest in collection and information handling technology.

b. continued rapid growth in collection capabilities with increasing emphasis on timeliness of processing.

c. responsive and dynamic tasking of collection systems in response to worldwide interests.

d. a centralized command, control, and communications (C3) system which is without precedent or rival.

e. a work force that is equally without precedence or parallel in terms of its professional credentials and training.

f. analytic tools which further amplify the capabilities of the work force.

g. reliable and competent allies with whom we are firmly linked in terms of our C3 intelligence systems.

h. an interaction with industry and academia on warning and intelligence problems in general, which forecasts continued rapid improvements.

Ivan might well conclude that the US system already has something like a Star-Wars level of technology: fast, centralized, cohesive, smoothly operating, and providing warnings and aiding executive response to events even before they reach crisis proportions.

Fundamental Doctrinal Problems

We must keep firmly in mind that indeed our capabilities have developed enormously and we have much to be proud of. But so much for role playing, and now for the rude awakening. There are fundamental doctrinal problems with which we confound our warning analysts.

First, we have a very inadequate understanding of what "warning" really is and how it differs from conventional intelligence analysis. One means of illuminating the distinction is to consider warning intelligence as having a focused goal which is the avoidance of harm; i.e., warning intelligence is that which is produced early enough concerning a potentially threatening situation to avert or ameliorate that forecast harm.

(b)(1)
(b)(3)(n)

Second, there is a series of paradoxes which make warning reporting an extremely tedious business. *Compartmentation* is closely tied to the problem of distribution. A report which takes into full account our most sensitive sources of information can be issued to very few people. Conversely, to issue a warning report to a broad audience one must restrict the use of all-source information, and thus an incomplete or inadequate warning may result. *Timing and probability* also work against one another. The nearer the possible event, the more likely we are to be able to accurately predict the probability of its occurrence. Conversely, to be able to avoid the harm implicit in the warning the earliest possible lead time must be given, which again is related to a lower level of confidence in the probability. *Coordination* should result in the most complete presentation of relevant material, and normally the highest confidence level in the probability of occurrence. However, coordination tends to suppress alternative analyses which may bode even more disastrous consequences for national security. Also, because our view of the future is perforce cloudy, it is hard to issue a coordinated warning sufficiently in advance of the event to ensure that the harm can be ameliorated.

Finally, our approach to the warning problem has been traditionally very narrow, i.e., equated to indications and warning which has historically been a military game, with specific focus on the military threat from Communist Bloc countries. We are beginning to understand that these military indicators cannot be viewed in isolation and indeed must be considered against the backdrop of the world political and economic situation. This broadened vision drives the complexity of the warning business to staggering dimensions.

Technological Implications

Let us now address the implications of our rapidly evolving technologies. The collection and processing technology which has given us an unequalled capability for reporting current events also has had a severe impact on our conduct of longer term analysis. Today's analyst is no longer allowed the luxury of analysis; he has been forced to become a data processor and a

current events reporter. First, the quantity of data collected, even though there is a significant amount of preprocessing, requires human review *before* becoming a part of a useful information resource. Second, the timeliness of the data, and the partially understandable demands of the users, i.e., the policymakers and planners, force the analyst into a reactive mode where reporting what has just happened takes on greater importance than estimating what may happen. The user does not consciously request this level of support, but through his actions and queries the analyst is forced into a defensive reporting role. In the "good old days" when analysts were working from fragmentary information, and tasking for confirmation took weeks, if not months, the analyst was forced to rely on his studied knowledge of his target to provide the best estimate of what might happen. Also because he had only limited, and not very timely, insight into what had happened there was no pressure to beat the New York *Times*. Again, working with limited and manageable inputs the analyst was able to build his own shoebox files which were considered to be not only adequate but the only responsive means to his historical information needs. As a side excursion, the analyst also did not have to worry about the security or integrity of his data base because it was under his physical control, and even the smallest data bases were large enough to be visible when removed from the premises.

But, along came that villain technology to destroy the idyllic analytic existence. Data began to pour in at an increasingly dizzying rate and analysts now could quickly task another sensor for confirmation or amplification rather than make a judgment about the possible consequences of the event. Therefore, why speculate, interpolate, or extrapolate? The data base building problem remained largely manual, at least to the extent of requiring significant human intervention, but because of the size of these bases additional analysts were assigned to do nothing else. The target analyst lost control and often even access. Undaunted, our clever analysts often recreated their own pieces of the data base, which caused problems in redundancy and inconsistency. Yet we continued to improve our collection systems at an increasing pace. There were constant collection inadequacies noted. We needed systems to see through walls and hear under water. The communications spectrum grew and, as is always the case, the new spaces filled with data. We used these new communications capabilities to ensure that the data arrived at our analyst's desk instantly.

But alas, how was the technology helping the analyst, other than providing him with more data to process and less access to information? The terminal arrived to replace the morning pile of messages and occasionally to replace his pen and paper. A few "automated" data bases became available, but these were often known for the difficulty of access and were rarely available from a local terminal. To ensure access to more than one source of information the analyst was required to learn the vagaries of each and every system to which he required access.

What went wrong? Should we not have focused on improved collection? Were we not right in waiting for the perfect solution to the analyst's problems? The answers are not clear cut. But rather than dwell on what went

wrong, let us consider what opportunities there are to meet the challenges of this era in information handling.

Today, technology is not a problem; the rapid advancements in storage, processing, and display technologies virtually assure us of being able to meet the analyst's requirements *if* they can be adequately defined and understood. The problem today is one of cognitive analysis, understanding how the analyst does or should function and then providing the tools which will provide the analyst access to the information and the necessary analytic routines.

Will our current evolutionary approach do the job? I do not believe so. Continuing to use the current analytic model will result in improvements in the basic tools for processing, but will only make the analyst a better processor of data, not a better analyst of information. A new approach must be formulated which begins with the collection systems, viewing the stream of data as something which wherever possible must be changed into useful information *before* being provided to the analyst

(b)(1)
(b)(3)(n)

The challenge, then, is not just to automate the way the analyst does his business today, but rather to analyze the basic functions of the analyst and develop new means of working with the information base necessary and pertinent to the task.

Training

In scoping the responsibilities of the National Intelligence Officer for Warning, Mr. Casey and I agreed that it was the problems of process that should be addressed, and so I have undertaken initiatives in the following areas.

The training requirements inherent in the technological revolution lag in many respects. Particularly at the middle levels of management and analysis, personnel are no longer familiar with the crises of the past and their inherent lessons to be learned. They are swept up in the daily routines of processing and current intelligence reporting. Significant long-term analyses and projections are still being formulated but are often frustrated by outdated managerial understanding of the warning system or the warning process in general. Traditional forms of analysis cannot compete with the data flood. Our abiding concern to be right has made us unduly wary of "false alarms" and the so-called "cry wolf" syndrome. The result is that good analysis is lost with the bad

and daring insights and projections never surface for analysts' fear of being wrong, or they are too late to be of use except in hindsight.

We are trying through dialogue with both the intelligence and operational communities to develop a fuller and more subtle understanding of the use of warning by those fulfilling different roles in the decision-making chain. This requires new definitions and tools for warning based on a better understanding of how people react to threats.

We have also established a program of community seminars to review warning problems and possible solutions. The primary purpose is to spread awareness of these problems among senior analysts and users and hope that they are able to convey the gospel within their agencies and departments. We are gaining valuable insights and notions of possible corrective actions from this sharing of ideas and experiences.

We have established a Warning Training Working Group comprising representatives from the Defense Intelligence College, Central Intelligence Agency, and the National Cryptological School to deal with the training requirements for national warning. This group is currently developing a warning syllabus which will form the basis for new courses and be integrated into existing courses. It is hoped that this syllabus can also form the outline for a "warning primer" which could be used for senior level policy officials who are not, but must become familiar with the warning community, its procedures, and its products.

We are beginning a program with the Army War College which we hope will expand to the other service schools. Our intent is to foster a level of academic research at the service schools which will expand our mutual understanding of the warning problems.

The art form for warning reporting needs a considerable amount of attention. The only "official warning" vehicle is the alert memorandum, which suffers from a bad reputation and disuse. Our discussions with Mr. Casey and with community analysts and reporters lead us to the conclusion that some form of warning memorandum may be required. It must have a great flexibility to allow for any level of coordination and stimulation from any level of the intelligence community. As with any warning vehicle, it must take into full account the viability and importance of the "old boy network." A direct call from the DCI to the Chairman of the Joint Chiefs will always carry more credibility than a formal memorandum to a community of recipients.

Operations and Command Centers are a significant part of the warning apparatus. Most important is the recognition that as a network they have a capability that far transcends the sum of each of their individual capabilities. In 1983 the chiefs of the Washington area centers met with me (b)(1) for a two-day conference. The dialogue was extremely good and a number of actions have sprung from that meeting to include upgrades to existing communications capabilities, the development of tailored training programs, and the development of a fiscal program for network enhancement and training.

Other initiatives are in the talking stages to include looking at reporting media for warning; studying the applicability of disaster theory to warning; expansion of the Worldwide Indications Monitoring System to a national system including political and economic indicators; bringing our allies more closely into our warning system.

For the future, many of the problems I have discussed will intensify. But we must avoid locking our understandings of warning into a straitjacket of the familiar. New understandings will be generated by new technology and new crises. These represent opportunities for intelligent integration of automated processing and manpower. Integration may require reorganization of the way all of us do business. We must identify and foster genuine analysis, not just information processing by our analysts. The automated tools will arrive, but they must aid the analyst, not just complicate his job or narrow his vision.

The Department of Defense has never lost its focus on the need for warning. Indeed, the DIA has been in the forefront of the development of indicator methodologies, and now the message is spreading into other areas of government. But even the Department of Defense systems must continue to evolve. We must remember that the answers developed after Pearl Harbor were suitable for that era but are totally inadequate today. Tomorrow brings only more challenges and opportunities. Fortunately, the warning community is stretching its limbs and is awake.

This article is classified ~~SECRET~~.